adaptiva

# Top Five Security Best Practices for Windows 10 in the Enterprise

# Table of Contents

Introduction ..... 3
UEFI with Secure Boot ..... 4
Tips for Implementing UEFI with Secure Boot ..... 4
Credential Guard ..... 5
Tips for Implementing Credential Guard ..... 6
Device Guard ..... 7
Tips for Implementing Device Guard ..... 8
BitLocker ..... 9
Tips for Implementing BitLocker ..... 10
Windows Information Protection ..... 11
Tips for Implementing Windows Information Protection ..... 12
Other Windows 10 Security Features ..... 13
The Importance of Maintaining Good Security Practices when Migrating to Windows 10 ..... 14
Boost the Endpoint Security Power of SCCM ..... 14
Safeguard SCCM Environments from Cyberattacks ..... 14
Speed Real-time Responses to SCCM Threats ..... 14
Find Out More ..... 15
About Cliff Hobbs and FAQShop.com ..... 15
About Adaptiva ..... 15
Appendix A: Useful Links ..... 16

# Introduction

A recent survey conducted by Adaptiva[1] found that 70% of Enterprise IT companies are concerned about security in their environments with the overwhelming majority of respondents planning to conduct security audits this year.

Respondents were also concerned about potential vulnerabilities in their environments but were optimistic that a move to Windows 10 could make their enterprises more secure.

Windows 10 is Microsoft's latest and most secure operating system (OS) to date. It has to be. The ever increasing complexity, adoption and use of technology enriches our lives and can make them easier, but with this comes an ever increasing spectrum of attack vectors.

Microsoft has broken these down into the following three broad categories in Windows 10:

- **Identity and access control –** Users presenting an identity to a system to perform an action, the system verifying that the user is valid, and the system then determining if the user has the relevant level of access to perform the requested action.

- **Information protection –** Windows 10 can separate personal versus company data and applications into containers. Then it can encrypt the company information and apps, prevent data leakage to personal locations (email, cloud), and protect data when shared.

- **Malware resistance –** With the majority of attacks being performed by ever adapting, automated software attacking our systems (rather than the spotty teenagers in the 1980s), we need several lines of defense. From ensuring the start up process is clean through to ensuring we are booting into a clean, secure operating system the right way. The old adage "*prevention is better than cure*" is the buzzword for this.

With all these powerful new security features in Windows 10, trying to decide which features to implement and how to implement them might seem intimidating.

The purpose of this document is to provide you the reader with the Top 5 Security best practices for Windows 10 in the enterprise.

Although the term "*Top Five*" is used, it does not mean that any item is any more importance than any of the other items. Of course, the Top Five in your company may differ based on needs. Windows 10 also includes a host other security and non-security related features not covered by this whitepaper which you can read more about at:

https://www.microsoft.com/en-US/windows/features

# UEFI with Secure Boot

Few people think about what happens when they turn on their PC, they just hit the power button. Part of the boot process involves the PC looking for a bootloader which is then simply used to load the operating system. What if the bootloader has been tampered with or indeed the operating system? Without any safeguards in place the PC could be booted into an infected/rogue operating system.

To prevent this the Unified Extensible Firmware Interface (UEFI) specification was devised. It is a specification for a software program that connects a computer's firmware to its operating system (OS), which basically replaces the old Basic Input Output System (BIOS) traditionally used on PCs.

In addition to UEFI, the Secure Boot security standard was developed by members of the PC industry to help make sure that when your PC boots, it only uses software trusted by the PC manufacturer.

When the PC starts, the firmware checks the signature of each piece of boot software, including firmware drivers (Option ROMs) and the operating system. Only the hardware manufacturer has access to the digital certificate required to create a valid firmware signature. If the signatures are good, the PC boots and the firmware gives control to the operating system.

# Tips for Implementing UEFI with Secure Boot

### Tip 1 – Look for BIOS Upgrades on older machines

Secure Boot was originally introduced in Windows 8. If your computer did not ship with Windows 8/10 you still may be able to use it by updating the BIOS. Contact your computer manufacturer to see if a BIOS update is available that will enable this.

### Tip 2 – Review Adaptiva's Free ConfigMgr Solution

If you use Microsoft's System Center Configuration Manager (ConfigMgr), then take a look at Adaptiva's free ConfigMgr Community solution that will help you automate migrations from Windows 7/8 to secure Windows 10:

http://www2.adaptiva.com/l/139131/2016-07-18/j7lfk

Not only does this provide you with an automated, unattended solution using ConfigMgr and freely available vendor utilities, it also handles the deployment of secure Windows 10 Enterprise with Secure Boot. It does not require any Adaptiva software to function, just straight ConfigMgr.

### Tip 3 – Take care if you need to Disable Secure Boot

You may have the requirement to disable Secure Boot. For example, you might want to run an unsigned operating system, or use hardware that is incompatible with Secure Boot. All PCs certified to run with Windows 8 and later allow you to disable Secure Boot, but there a few things to bear in mind:

- You may need to restore your PC to its factory state in order to re-activate Secure Boot if you disable it and then install other hardware and software.
- With Secure Boot disabled you are at greater risk from bootkit infections as your PC just runs the bootloader without verifying it in any way.
- You need to access the BIOS in order to disable Secure Boot. Take care you don't make any other changes to the BIOS that could prevent the machine from booting.

If you do need to disable Secure Boot, Microsoft provides details on how to do so here.

## Credential Guard

Credentials are key to controlling and gaining access to systems. However, they can also be easily compromised and once that happens you could be in big trouble. What if there were a way to better protect your credentials built-in to the operating system and to prevent operations if something untoward is detected?

Virtualization technologies such as Microsoft's Hyper-V are not new, and segregating operations to specific virtual machines is an effective way to reduce contagion. So what if we could leverage this same technology to isolate core operating system services in a similar way but in a client operating system such as Windows 10?

Well in Windows 10 you can. This is known as virtualization-based security (VBS), which means even if the kernel mode of the host operating system is compromised, the core operating system services cannot be manipulated.

This VBS environment consists of two services. The Hypervisor Code Integrity (HVCI) service determines if code executing in kernel mode is trustworthy and securely designed. The Local Security Authority (LSA) service manages authentication operations, including NT LAN Manager (NTLM) and Kerberos mechanisms.

In a nutshell Credential Guard segregates a part of the LSA service to help mitigate *pass-the-hash* and *pass-the-ticket* attacks. A pass the hash attack is where an attacker uses the underlying NTLM and/or LanMan hash of a user's password to authenticate to a remote server/service instead of requiring the actual password. A *pass-the-ticket attack is* where an attacker uses the Kerberos Ticket Granting Ticket of a user recently logged into the domain to authenticate to a Windows server, gaining access to all servers and other resources for which the user has priviledges.

As Rob Lefferts, Director of Program Management, Windows Enterprise and Security states:

*"Credential Guard has proven so impactful that customers have told us that it's their top-priority security feature and a benefit that is so compelling that it justifies the Windows 10 deployment all by itself. It's no wonder, since it combats one of the most prolific and critical tactics being used against organizations today: Pass the Hash (PtH)."*

In order to use Credential Guard you are going to need the following combination of hardware and software:

- **Hardware**
    - UEFI firmware version 2.3.1 or higher and Secure Boot
    - Virtualization extensions
        - Intel VT-x or AMD-V
        - Second Level Address Translation (SLAT)
    - A VT-d or AMD-Vi IOMMU (Input/output memory management unit)
    - Trusted Platform Module (TPM) version 1.2 or 2.0
    - Secure firmware update process

  - Firmware updated for Secure MOR implementation (required to help prevent certain memory attacks)
  - Physical PC if you are running Windows 10 version 1507 or 1511
  - Virtual machine (Generation 2) if you are Windows 10 version 1607.

- **Software -** The x64 version of Windows 10 Enterprise running the Windows hypervisor.

## Tips for Implementing Credential Guard

### Tip 1 - Use the Device Guard and Credential Guard hardware readiness tool

Microsoft have released the **Device Guard and Credential Guard hardware readiness tool** (https://www.microsoft.com/en-us/download/details.aspx?id=53337) which you can use to check if your hardware is ready for Credential Guard (and Device Guard). The tool can enable them as well.

### Tip 2 – Keep Your Firmware Updated

As Credential Guard relies on the security of the underlying hardware and firmware it is vital that you keep your firmware updated with the latest security fixes. You can use the System.Fundamentals.Firmware.UEFISecureBoot Windows Hardware Compatibility Program requirement to verify your firmware complies with the secure firmware update process.

### Tip 3 – Verify your Firmware

You can use the System.Fundamentals.Firmware.CS.UEFISecureBoot.ConnectedStandby Windows Hardware Compatibility Program requirement to verify your firmware is using UEFI version 2.3.1 or higher and Secure Boot.

# Device Guard

Historically, users have by and large been rather too trusting when running applications. If an application causes damage or allows a security breach, system administrators find out after the fact.

In Windows 10 this all changes with the Device Guard feature, the basic premise of which is to only run those applications we know about and explicitly trust. Anything else will be blocked.

Device Guard is a combination of hardware and software hardening features that utilize the new virtualization-based security (VBS) environment introduced in Windows 10 discussed in the Credential Guard section.

On the hardware side, Device Guard integrates with advanced hardware features such as CPU virtualization extensions, Input–Output Memory Management Units (IOMMUs), and 64-bit processors with Second Level Address Translation (SLAT), to leverage these hardware features inside Windows 10 itself.

As a result, in order to use Device Guard you are going to need the following combination of hardware and software:

- **Hardware**
    - UEFI Secure Boot (optionally with a non-Microsoft UEFI CA removed from the UEFI database)
    - Virtualization support enabled by default in the system firmware (BIOS):
        - Virtualization extensions (for example, Intel VT-x, AMD RVI)
        - SLAT (for example, Intel EPT, AMD RVI)
        - IOMMU (for example, Intel VT-d, AMD-Vi)
    - UEFI configured to prevent an unauthorized user from disabling Device Guard–dependent hardware security features (for example, Secure Boot).
- **Software -** The x64 version of Windows 10 Enterprise with kernel mode drivers signed and compatible with hypervisor-enforced code integrity.

Utilizing Device Guard, organizations can chose exactly which software (either from external suppliers or written in house), can run code on your Windows 10 clients. If it's not on the list, the machine can't run it. In this way, it protects the system core and the processes and drivers running in kernel mode.

Device Guard can be enabled and managed using the following management tools:

- **Group Policy -** Windows 10 includes an administrative template you can use to configure and deploy the configurable code integrity policies for your organization.
- **System Center Configuration Manager –** ConfigMgr can simplify the deployment and management of both catalog files and code integrity policies, as well the management of hardware-based security features. It can also provide version control.
- **MDM systems -** Microsoft Intune and non-Microsoft MDM systems can be used to deploy and manage code integrity policies and catalog files.
- **Windows PowerShell –** PowerShell is primarily used to create and service code integrity policies.

# Tips for Implementing Device Guard

### Tip 1 – Deploy Device Guard along with other threat-resistance features in Windows 10

Device Guard is not meant to be the silver bullet to all your anti-malware issues. To get the most from it you should deploy it along with the other threat-resistance features available in Windows 10 such as AppLocker and Credential Guard. Microsoft also recommends you continue to maintain an enterprise antivirus solution as part of your enterprise security portfolio.

### Tip 2 – Determining which Dell and Lenovo Models support Device Guard

A lot of the security features mentioned in this whitepaper rely on the Trusted Platform Module (TPM).

You can use the table in the **Dell Platform Support for TPM 2.0 (Shipping as of January 2016 - Factory default is TPM 2.0 for Windows 10)** section of the TPM 1.2 vs. 2.0 Features page of the Dell Wiki to verify to see which Dell systems support TPM 1.2/2.0.

For Lenovo machines they added the Device Guard feature to their 2016 ThinkPad models (T460/X260) which feature Intel's Skylake platform. They added the Secure Boot feature to their 2014 ThinkPad models (T440/X240) which feature Intel's Haswell platform.

## BitLocker

Any data stored locally on a machine is at risk especially when that machine leaves the sanctuary of your company. There are various steps you can take to protect the machine and its data including encrypting the hard drive, which is where BitLocker comes in.

BitLocker is at its most effective when it is used on a machine with a Trusted Platform Module (TPM) chip. The chip works with BitLocker to help protect the user's data and ensure the system was not interfered with with while offline.

Enabling the TPM in earlier versions of Windows was a bit of a hassle. Thankfully in Windows 10 Microsoft now includes instrumentation that allows the operating system to fully manage the TPM. This means no more messing about in the BIOS and countless restarts.

In Windows 10 BitLocker has had a bit of an overhaul. It can now protect individual files as well as entire hard drives (both system and data). It is also now possible to pre-provision BitLocker (enabling the TPM and BitLocker), using a Task Sequence or from within the Windows Pre-installation Environment before installing Windows. If you also configure BitLocker to encrypt Used Disk Space Only this can drastically reduce the time taken to enable BitLocker compared to previously where you had to wait for the entire drive to be encrypted before BitLocker was fully enabled.

A word of warning here. If you are encrypting a drive using Used Disk Space Only on a disk that previously contained confidential data that has since been deleted, the confidential data is potentially at risk of being able to be recovered by recovery tools. This risk may remain until the space it occupies is overwritten by fresh data which will be encrypted by BitLocker.

Of course there will be a slight performance overhead of data being encrypted as it is being written to unencrypted parts of the disk.

What else can you do if someone manages to get physical access to the machine? If your machine has a TPM and BitLocker has been enabled on the system drive, you can enforce that the user needs to type a PIN before BitLocker will unlock the drive. They then also need to have valid credentials to able to logon to the machine.

Enabling such an option is a case of balancing the risk versus the impact it is going to have on the user who has to remember and type the PIN each time they want to use their machine. Users can now manage their PINs and passwords in Windows 10 themselves rather than having to contact a system administrator or use an administrative account.

There are a whole raft of other improvements to BitLocker in Windows 10 such as support for Self-Encrypting Drives (SEDs) and Network Unlock. These capabilities are a bit beyond the scope of this paper, but worth checking out if interested.

# Tips for Implementing BitLocker

### Tip 1 – Tie your User Credentials to TPM to prevent Brute Force Attacks

With BitLocker enabled to protect the system drive, consider tying your users credentials to TPM. This way, if someone enters them incorrectly a set number of times (such as during a brute-force attack), Windows will automatically restart the device and put it in BitLocker recovery mode where it will stay until someone enters a valid 48-character recovery key. Obviously, make sure you have copies of your Recovery keys.

To establish how many incorrect guesses you want to allow, run **gpedit.msc** to open the Local Group Policy Editor. Then navigate to:

**Computer Configuration\Windows Settings\Security Settings\Security Options.**

Open the **Interactive Login: Machine Account Lockout Threshold** and set the number of **invalid logon attempts** to the required value.

### Tip 2 – You don't need to Decrypt a Windows 7/8 machine to remove BitLocker in order to upgrade it to Windows 10

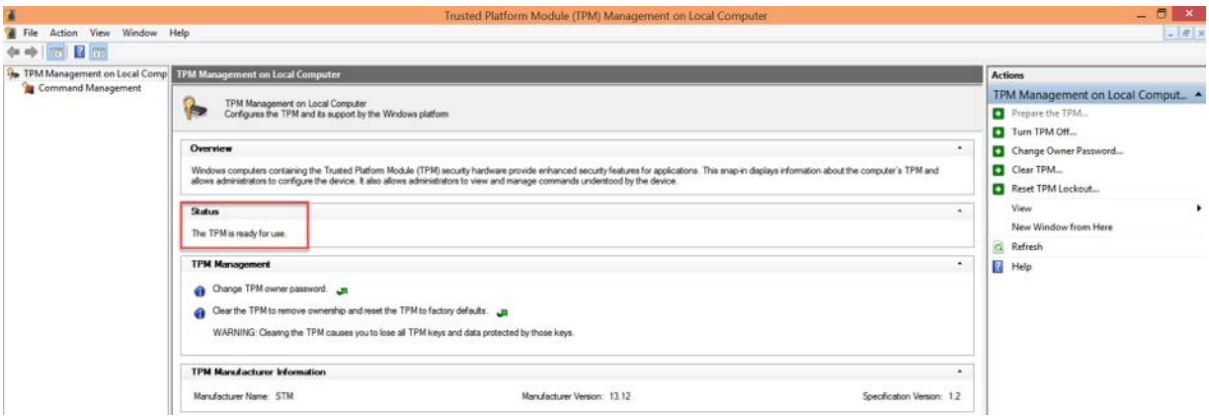
If you already have BitLocker enabled on Windows 7/8 machines you don't need to decrypt the drive (i.e., completely remove BitLocker protection and fully decrypt the drive), in order to upgrade the machine to Windows 10.

Instead, open the **BitLocker Drive Encryption** Control Panel. Then click **Manage BitLocker** and click **Suspend** which simply disables BitLocker authentication and instead uses a clear key on the drive to enable access (the drive is not decrypt).

Once you have completed the upgrade to Windows 10 open Windows Explorer, right-click the relevant drive and click **Resume Protection** to reapply the BitLocker authentication methods and delete the clear key.

### Tip 3 – Run "tpm.msc" to verify if a computer has a TPM

To verify if a computer has a TPM chip simply open the **Trusted Platform Module (TPM) Management Console** (run **tpm.msc**) and look under the **Status** heading. It will state **The TPM is ready for use** if the computer has a TPM and it has been prepared.



## Windows Information Protection

Even given the long history of the PC and Windows, there are still several missing pieces of the security jigsaw including:

- No ability to prevent scenarios such as users leaking corporate data to non-corporate email addresses (such as personal ones or even worse to the wrong address).
- No cure for the headache of wanting to move to Bring Your Own Device (BYOD), but being unable to first contain data on the device and then, if required, securely wipe it should the need arise.
- Cannot prevent users from copy and pasting corporate data into the wild via social media and other channels.
- No easy way to restrict business data so it is contained only to specific, authorized business applications.

However, it is not all about restriction. Many businesses rely on being able to share business information securely both inside their organization and outside.

Up until now none of the required functionality to tackle these issues has been built into the Windows operating system *out-the-box*. Sure Microsoft provides some tools to address some of these areas but not all of them.

However, now with the advent of the Windows 10 Anniversary Edition Microsoft provides these capabilities and more in the Windows Information Protection (WIP), feature formerly known as Enterprise Data Protection.

Specifically designed to work with Office 365 ProPlus and Azure Rights Management, WIP can distinguish between corporate and personal data. Then it can restrict what happens to corporate data when it leaves the device. For example a user can be prevented from forwarding an email containing business data to an unapproved recipient. At an even more basic level, WIP can control which applications have access to corporate data and what those applications can do with it. For example, WIP can prevent the copy and pasting or printing of corporate data in unapproved applications or to unapproved locations. If a user tries to perform an action that is not permitted, the action can be blocked and audited. This auditing can highlight potential issues that may need further attention, such as education on corporate policy.

Traditionally, solutions to issues such as these have required compromising the user experience at the expense of securing the data. There are countless Mobile Device Management (MDM), solutions available, all with their nuances such as requiring the user to switch modes depending on whether they are working with corporate or personal data as these are kept in separate containers. With some solutions, the user can't use Outlook but instead has to use a specific MDM email client which is stripped down in terms of functionality for security reasons.

In the non-mobile space, things are slightly better and more integrated with the operating system. However, companies are still relying on third party add-ons which they need to purchase, learn, and maintain.

WIP on the other hand is part of the Windows OS itself so it's fully integrated. It is also incredibly easy to deploy by enabling some policies in your MDM (for example Microsoft Intune) or using System Center Configuration Manager (ConfigMgr). As WIP is fully integrated into the OS there is no need to switch modes to work with different data types, or to use feature-limited versions of applications. Users just carry on doing what they do using the applications they know. WIP can even continue to protect your data when it is copied off to USB drives or other removable data.

Microsoft's goal when designing WIP was to come up with something that everyone could and would deploy regardless of company size. As it works in conjunction with Office 365 and Azure Rights Management this is one Windows 10 feature you definitely want to look at to take your data leak prevention to the next level.

## Tips for Implementing Windows Information Protection

### Tip 1 – Ensure you are using Office 2016

If you want to be able to use WIP with Office, ensure you are using the Office 2016 Universal Windows apps as these are ready to go and fully support WIP.

### Tip 2 – Check out the following Microsoft Resources

Microsoft publishes a whole host of information about WIP, including how to set it up. Here are a couple of links to get you started:

Create a Windows Information Protection (WIP) policy:
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/overview-create-wip-policy

General guidance and best practices for Windows Information Protection (WIP):
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/guidance-and-best-practices-wip

### Tip 3 – You only need Windows 10 Professional SKU and upwards to get WIP

Although it may seem like you need the Enterprise version of Windows 10 in order to get access to Windows Information Protection (WIP), that is not the case.

WIP is available in the Windows 10 Professional SKU and upwards as detailed under the **Security** section of the Compare Windows 10 Editions page on the Microsoft website.

## Other Windows 10 Security Features

In addition to the Top Five Security features we've already looked at in this document, Windows 10 includes a plethora of other security-related features some of which are summarized below:

- **Early Launch Antimalware (ELAM) –** ELAM designed to allow the antimalware solution to start before all non-Microsoft drivers and applications. This way, it can prevent malware from updating/ replacing a non-Microsoft–related driver that starts during the Windows start-up process. ELAM is supported by Windows Defender in Windows 10, System Center 2012 Endpoint Protection, and other 3rd party antimalware applications.

- **Microsoft Passport –** Provides strong two-factor authentication (2FA), fully integrated into Windows. Microsoft Passport replaces passwords with the combination of an enrolled device and either Windows Hello (see below) or a PIN. Conceptually, Microsoft Passport is similar to smart cards but without the need for a Public Key Infrastructure (PKI).

- **Network Unlock –** Allows BitLocker-protected PCs to automatically start whenever they are connected via a wired connection to a corporate network on which Windows Deployment Services (WDS) runs, and then prompt the user for a PIN to unlock the drive (assuming you have enabled PIN-based unlock).

- **SmartScreen -** A technology designed to help prevent Windows devices from ever coming in contact with threats. If an Internet Explorer or Edge user visits a site that Microsoft knows is malicious, it will alert the user AND hopefully stop them going there. In the Windows 10 Anniversary Update, SmartScreen is powered by the Microsoft Intelligent Security Graph giving broader reach AND faster reputation classification for emerging threats.

- **Windows Hello –** The new built-in biometric sign-in option for Microsoft Passport which allows users to unlock their devices using facial or fingerprint recognition. Once unlocked authentication to the device and its resources is facilitated through a mixture of the user's unique biometric identifier and the device.

- **Microsoft Edge –** Microsoft has made improving browser security with Microsoft Edge, a browser that is a Universal Windows app fundamentally compartmentalized which runs in an AppContainer that sandboxes the browser from the system, data, and other applications. Built from the ground up, Edge is more secure as it is 64-bit and does not support non-Microsoft binary extensions. It also simplifies security configuration tasks as it uses a simplified application structure and a single sandbox configuration. Plus Edge's default settings align with security best practices therefore making it more secure by default.

# The Importance of Maintaining Good Security Practices when Migrating to Windows 10

As with any migration, when considering migrating to Windows 10 you need to plan your migration carefully to avoid as many potential issues as possible.

Of course Microsoft's recommend tool of choice when it comes to deploying/migrating to Windows 10 is System Center Configuration Manager (ConfigMgr) Current Branch which includes a raft of functionality.

But in addition to ConfigMgr, you may also wish to take a look at Adaptiva's OneSite product, which includes features such as the following to bolster and improve on the ConfigMgr *out-the-box* experience in three key areas:

- Boost the Endpoint Security Power of SCCM
- Safeguard SCCM Environments from Cyberattacks
- Speed Real-time Responses to SCCM Threats

## Boost the Endpoint Security Power of SCCM

This is all about achieving secure content delivery, anytime, anywhere. It shouldn't matter what you need to deliver, to where, or when; OneSite can deliver content promptly, securely and without adversely affecting the core purpose of your network – your business.

## Safeguard SCCM Environments from Cyberattacks

It is all very well being able to deliver content efficiently, but if the content is not secure and is open to tampering either in transit or at its destination then you have big problems. OneSite can drastically reduce your ConfigMgr infrastructure requirements and thus your potential attack surface and the headaches of monitoring and maintenance. Not only is all content sent by OneSite encrypted during transmission, it's also securely encrypted on the disk.

Couple this with the use of 512-bit Secure Hash Algorithm (SHA-512) to prevent tampering, and OneSite meeting all the requirements for the Federal Information Processing Standard (FIPS) Publication 140-2 (amongst others), means OneSite delivers the highest security compliance of any content distribution technology in market.

## Speed Real-time Responses to SCCM Threats

Should the worst happen and you find yourself with a security breach you want a solution that is "*ready to go*" with the most secure configurations (that can be customized). You also want the ability to remediate the breach as soon as possible by pushing the required fix out once to all affected endpoints without waiting for each individual client to reach it's polling cycle. With OneSite, you can also use the Workflow Designer to enforce security policies and lock down errant systems automatically.

## Find Out More

For more information on any of the above, see **SCCM and Endpoint Security** at https://adaptiva.com/sccm-endpoint-security

## About Cliff Hobbs and FAQShop.com

This report was written by Cliff Hobbs. Cliff is a 13 times Microsoft Most Valuable Professional (MVP), the first to be awarded in the UK for Microsoft System Center Configuration Manager (ConfigMgr/SCCM) and Systems Management Server (SMS).

He has worked as a Consultant with the product since 1998, during which time he has gained extensive experience of designing, deploying, supporting, and documenting enterprise-wide Configuration Manager implementations on behalf of many companies such as Microsoft, HP, EDS, Getronics, 1E and Abbey (now Santander), across multiple industry sectors.

Since 1998 Cliff has been writing Frequently Asked Questions (FAQs) related to ConfigMgr and its related products. In 2003 he founded http://faqshop.com which is one of the most popular websites for ConfigMgr-related information.

## About Adaptiva

Adaptiva is a leading, global provider of IT systems management solutions that advance the power of Microsoft System Center Configuration Manager. Founded in 2004 by the lead architect of Microsoft SMS 2003, Adaptiva enables IT professionals to securely speed enterprise-wide software deployments without adding costly servers or throttling network bandwidth. The company's breakthrough peer-to-peer systems management technology uses intelligence, automation, and bandwidth optimization techniques to distribute content faster than any other systems management solution available today. Adaptiva's suite of smart scaling systems management products includes OneSite™ for rapid content distribution and management, Client Health™ for endpoint security, troubleshooting, and remediation, and Green Planet™ for energy-efficient power management and patching. The company's software is used by Fortune 500 companies and deployed on millions of devices in over 100 countries. Learn more at adaptiva.com.

# Appendix A: Useful Links

This Appendix contains both links used as information soures for this whitepaper, as well as those the author feels are useful to help you learn more about Security in Windows 10.

**Advancing Security for Consumers and Enterprises at Every Layer of the Windows 10 Stack**

https://blogs.windows.com/business/2016/06/29/advancing-security-for-consumers-and-enterprises-at-every-layer-of-the-windows-10-stack/#PdO3I1L7RimdPZI8.99

**Community Options For Migrating from BIOS to UEFI and Secure Windows 10**

http://myitforum.com/myitforumwp/2016/07/22/community-options-for-migrating-from-bios-to-uefi-and-secure-windows-10/

**Compare Windows 10 Editions**

https://www.microsoft.com/en-us/WindowsForBusiness/Compare

**Device Guard and Credential Guard hardware readiness tool**

https://www.microsoft.com/en-us/download/details.aspx?id=53337

**Disabling Secure Boot**

https://msdn.microsoft.com/windows/hardware/commercialize/manufacture/desktop/disabling-secure-boot

**Free ConfigMgr Community Solution: Automate migrations from Windows 7/8 to secure Windows 10**

http://www2.adaptiva.com/l/139131/2016-07-18/j7lfk

**Introducing Windows Information Protection**

https://blogs.technet.microsoft.com/windowsitpro/2016/06/29/introducing-windows-information-protection/

**Microsoft Malware Protection Center**

https://blogs.technet.microsoft.com/mmpc/

**Post Breach Detection with Windows Defender Advanced Threat Protection**

https://blogs.technet.microsoft.com/windowsitpro/2016/06/29/post-breach-detection-with-windows-defender-advanced-threat-protection/

**Protect derived domain credentials with Credential Guard**

https://technet.microsoft.com/itpro/windows/keep-secure/credential-guard

**SCCM and Endpoint Security**

https://adaptiva.com/sccm-endpoint-security

**Secure Boot Overview**

https://technet.microsoft.com/en-us/library/hh824987.aspx

**What's new in Windows 10 security**

https://technet.microsoft.com/en-us/itpro/windows/whats-new/security

**Windows 10 security overview**

https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-10-security-guide